SecurityRisk ADVISORS

CyberSOC Threat Notification

Microsoft Exchange Server – Known Attacks

Executive Summary

On March 2, 2021, Microsoft released several security updates for Microsoft Exchange Server to address multiple remote code execution vulnerabilities that have been detected in targeted attacks. Microsoft recommends prioritizing updates on externally facing Exchange Servers. All affected Exchange Servers should be updated.

Description

Microsoft released out-of-band patches for the following vulnerabilities recently seen being exploited; CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. The attacks detected by Microsoft were used to access on-premises Exchange servers which provided access to email accounts and allowed the installation of additional malware to enable persistent access to victim environments.

Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to HAFNIUM, a group assessed to be state-sponsored and operating out of China.

HAFNIUM operators deployed web shells on compromised servers allowing the attackers to potentially steal data and perform other malicious actions.

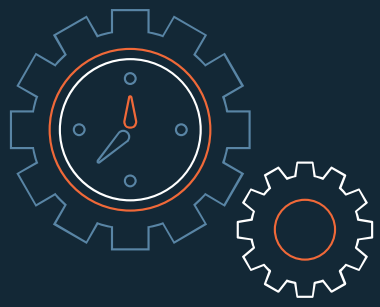
Affected Products

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

Microsoft Exchange Server 2010 is being updated for Defense in Depth purposes. Exchange Online is not affected.

Recommendations

Immediately apply the available patches from Microsoft, prioritizing updates on externally facing Exchange Servers, or temporarily disabling external access to Microsoft Exchange until a patch can be applied.



Vendor: Microsoft

CVE-ID: Multiple

CVE-2021-26855,
CVE-2021-26857,
CVE-2021-26858,
CVE-2021-27065

Published: Mar 2, 2021

CVSS V3 Overall score: 9.1, 7.8, 7.8, 7.8

Criticality: Critical, High, High, High

Patch Availability: Yes

Vulnerability Type: Remote Code Execution

Exploitability Metrics

Attack Vector: Remote, Local, Local, Local

Attack Complexity: Low

Privileges Required: None, Required, None, Required

User Interaction: None

Impact Metrics

Scope: Unchanged

Confidentiality: High

Integrity: High

Availability: None, High, High, High

Confidence Metrics

Exploitability: Functional

Remediation Level: Official Fix

Report Confidence: Confirmed

References

- https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
- https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901
- https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io